NetworkWorld Reprint

The leader in network knowledge ■ www.nwfusion.com January 12, 2004 ■ Volume 21 Number 2

Review

SSL VPN GATEWAYS

NetScreen, Nokia top the growing field of products that target simplified secure remote access

■ BY JOEL SNYDER, NETWORK WORLD GLOBAL TEST ALLIANCE

Security with ease of use is the promise of Secure Sockets Layer VPNs. In our test of seven SSL VPN gateways — from AEP, F5 Networks, NetScreen Technologies, Netilla, Nokia, Symantec and Whale Communications — we assessed how well each is equipped to provide secure remote access to corporate applications.

The good news is that several products are well-suited for enterprise use. Our World Class award goes to NetScreen for its outstanding application support, good access control mechanisms and overall interoperability. Nokia, Symantec and F5 all make our short list because of the broad spectrum of application support they offer.

Our basic assumption for testing SSL VPNs is that they must fit into existing networks and application environments (see How we did it, www.nwfusion.com, DocFinder: 9225).

To that end, we tested inter-operability of each device against 20 enterprise applications.

We tested these products from the point of view of network and security professionals; focusing heavily on access control and security features.

In terms of features, we evaluated auditing, accounting, re-porting and logging tools. We also tested client integrity scanners, which help ensure that virus scanners and firewall features are up to date.

Applications are everything

The biggest difference between SSL VPNs and traditional IP Security remote access VPNs is that the IPSec standard requires installation of client code on the end user's system, while SSL VPNs focus on making applications available through any Web browser.

In some cases, SSL VPNs must provide secure access to the applications that are served up as static Web pages on HTTP servers, but taking Web traffic in one port and sending it out another is not where these products bring their greatest value. SSL VPNs are deployed for bigger, more compelling reasons such as complex application translation of Web-to-e-mail servers, corporate directory and calendar systems, e-commerce applications, file sharing, and remote system management.

When it comes to proxying and application translation (see "SSL terms and conditions," page 3), we found big differences between products (see graphic, page 2). AEP and Whale were the weakest in this area, supporting the smallest number of application translators and proxies. Nokia was the only one of the stronger products to support application translation for FTP, Network File System (NFS) and Microsoft file servers. With F5, Netscreen and Symantec each offering a subset of the three. Netilla was the only offering to include translation for both Windows Terminal Services and a extensive array of terminal emulators, including telnet, Secure Shell (SSH) and IBM 3270. We tested all but the IBM emulations and had good results. F5 and NetScreen also included terminal emulator support for telnet and SSH, but they struck out because their emulators didn't work more than 25% of the time.

Because the products we tested offer such a variety of options, for you to pick the right gateway for your network you'll need a firm understanding of which applications you need translation for and be able to rank them in terms of importance. For example, Symantec and F5 gateways include e-mail application translation — so users can read and send mail via an application running on the gateway. Unfortunately, Symantec's built-in Web mail feature doesn't work if you have a lot of mail in your mailbox.

Even SSL VPN gateways that don't support a built-in Web mail tool would let you connect to a corporate messaging application,

Lining up proxy and application translation support

Support for Web applications, application translation of file servers and application translation of mail, terminal services and remote hosting access (Telnet and SSH) varies across applications. This chart only indicates claimed support, not the results of our interoperability testing.

	Web		File services			Other common applications			
	HTTP	HTTPS	FTP	CIFS	NFS	Web mail	Web terminal services	Web telnet	Web SSH
AEP	✓						✓		
F5	✓	✓		✓	✓	✓		✓	✓
NetScreen	✓	✓		✓	✓			✓	✓
Netilla	✓	✓		✓			✓	✓+	✓+
Nokia	✓	✓	✓	✓	✓				
Symantec	✓	✓	✓	✓		✓			
Whale	✓	✓		✓					

✓ Supports ✓+ Supports basic and additional applications

such as Microsoft Outlook Web Access, IBM's iNotes or the open source SquirrelMail. As our interoperability testing indicates, these rich applications have their own problems. So you might be left with the difficult choice of a rich Web-based messaging application that not everyone can use, or a less powerful and feature-poor Web mail system that is friendlier to unusual or older browsers.

Some applications cannot be translated, and SSL VPN gateways have two mechanisms for getting direct access into the network: port forwarding and network extension. Port forwarding lets you protect well-behaved applications on known servers, and network extension gives broader access via tunneling to an entire network.

The further down this direct access path you go, though, the more complicated and risky your SSL VPN deployment will be. To accomplish port forwarding or network extension, the SSL VPN gateway must push out software to the end user's workstation. This raises browser compatibility issues, operating system problems and security concerns. For example, a user sitting in front of Microsoft's Internet Explorer with browser security set to "high" would not be able to use any of these features. Unfortunately, permissions to lower browser security are not always available.

A second problem with port forwarding and network extension is security. One promoted strength of SSL VPNs is the ability to look into the application layer and give detailed access control to the network manager. When port forwarding and network extension come into play, SSL VPNs no longer offer such access control to applications because they are no longer aware of the underlying application. Rules down to the URL level, one of the characteristics of SSL VPN technology, aren't available when using network extension and port forwarding.

All the SSL gateways we looked at except for AEP and Netilla provide some port-forwarding functionality (see graphic, page 3). However, port forwarding is not sufficient for all applications. A good example is FTP, which uses IP addresses and port numbers within the protocol to identify a server and client socket for data transfer. Port forwarding won't work with all FTP clients, unless the SSL VPN gateway knows that it is forwarding FTP traffic and rewrites IP addresses within the traffic.

Application layer gateways(ALG) could add this kind of knowledge to port forwarding, and they are common in real firewalls. SSL VPN gateway vendors made an effort to add ALGs to their port forwarding to two areas: in e-mail, specifically MAPI (for Exchange clients) and Notes smarts, which ships with the NetScreen, Nokia and Symantec gateways; and in remote desktop clients using Citrix terminal services, which ships with NetScreen and Nokia gateways.

Instead of making port forwarding smarter with ALGs, many SSL VPN gateway products support network extension: connection of the end user's remote system to the network behind the SSL VPN gateway. In the group we looked at, all but Nokia and Whale include network extension technology.

E-mail is arguably the most popular SSL gateway feature because our testing found yet another way that some products support e-mail. AEP, NetScreen, Nokia and Symantec all include proxies for the standard mail protocols Simple Mail Transfer Protocol (SMTP), Post Office Protocol and Internet Message Access Protocol. The idea is that you'll point your POP or IMAP client mail application at the SSL VPN gateway, encrypting from client to the gateway using standard POP-over-SSL, IMAP-over-SSL and SMTP-over-SSL, thus adding security to the mail transactions. This technique also can add SSL to older mail servers or give access to servers that are on private address space. The benefit of using this technique is compatibility across all modern platforms and modern e-mail clients without requiring special operating system access the way port forwarding and network extension do.

Interoperability problems

Web applications are frightening things to security vendors. The extreme generosity of browsers in accepting and displaying incomplete Web pages, incorrect JavaScript and illegible Java has led to a generation of applications that make little sense from a software development point of view — but seem to work. Building an SSL VPN gateway to handle these applications is an unenviable task. We tested 20 applications with seven browser/ platform combinations and found wide variation in what works (see graphic, page 4).

One goal for this review was to test the vendors' claims that these products are easier to set up and use than IPSec VPNs. Along the way, we saw a lot of backpedaling: These products are easier for the end user to use, but sometimes harder for the network manager to maintain. In some cases, we know that updating client software, clicking hidden or obscure feature boxes, and a hefty dose of quality technical support could have solved the problems we saw. But we wanted to see how well the average network or security manager — not a Web application programmer — would do. We ruled out changes to client systems as unacceptable and not in the spirit of SSL VPNs' goal of security with ease of use.

We started with five basic Web applications, some of which included basic JavaScript. The only vendor to support five applications on seven platforms was Nokia, although F5 and NetScreen only missed one each, while Whale and Symantec missed three or less. AEP got bad marks on two of the applications, one with JavaScript and the other going to an SSL-protected Web server in the back — AEP doesn't support back-end servers with SSL, although everyone else does. Netilla also lost points for losing graphics. Although every page eventually loaded correctly if we pressed "Reload" enough, we gave Netilla only half-credit on applications that missed a lot of graphics the first time through.

Next up in our testing were the two big mail applications, Outlook Web Access 2003 and

Tracking port forwarding and network extension

We found problems in the port forwarding and network extension implementations in most of the products we tested. NetScreen worked the best in our tests, but spotty platform compatibility across all products makes this less than a guaranteed universal solution.

	Port forwarding		Network extension	
	Win3 2	Macintosh	Win3 2	Macintosh
AEP			✓	
F5	✔		✓	
NetScreen	✔	✓	✔	
Netilla			✔	
Nokia	✔	✓		
Symantec	✔		✓	
Whale	✓			

✔ Supports
✓ Supposed to work, but didn't in all our tests all the time.

iNotes, versions 6.0 and 6.5. Here, Nokia came closest to getting it right, with AEP and Symantec next in line (although Symantec did manage to crash our Netscape browser when feeding it iNotes). The newness of Outlook 2003 threw a bit of a curve at our SSL gateways. However, we argue that a big question for SSL VPNs is whether these products act like appliances, independent of the software behind them, or will they put you on a treadmill keeping things up to date?

It's pretty clear that vendors don't expect these gateways to work without some tuning. We restricted ourselves to out-of-the-box configuration, but most of the systems had a number of obscure knobs and adjustments that were added to help increase compatibility. Netilla is a good example. When defining an application, for example, you can select either "Fast HTML Translation" or "Full HTML Translation." The only documentation for how to choose one or the other is the ambigious note: "Fast is appropriate for most pages." As another example, Whale devotes 75 pages of documentation to fine-tuning the handling of applications .

Our third series of tests used three Web-based applications that included Java and different types of Flash. The results were dismal. F5, NetScreen and Symantec managed to each get one of the applications working some of the time. AEP, Netilla, Nokia and Whale scored zero in this phase. The lesson is simple: Advanced applications with tools such as Java and Flash just aren't going to work easily through SSL VPN gateways, not without using techniques such as port forwarding or network extension.

Our fourth set of tests looked at how these devices handled Microsoft, FTP and NFS file servers through application translation. Scoring this was tougher because not every device claimed to support all protocols. But we found products too smart for their own good. F5's snazzy tool for browsing file servers wouldn't work properly on our Safari browser; Netilla's tool wouldn't work properly on anything but Internet Explorer browser on Windows; and Whale couldn't handle older versions of Internet Explorer or Netscape.

We also managed to catch up both Nokia and Symantec with FTP server compatibility problems. When tested against a standard

SSL terms and conditions

The Secure Scokets Layer VPN market brings together many technologies to accomplish the goal of secure remote access. Understanding the strengths and limitations of SSL VPNs means knowing the meaning of four critical terms: proxying, application translation, port forwarding and network extension.

SSL VPN devices all start with at least one function: proxying Web pages. For the SSL VPN system that means connecting to a Web server, downloading a Web page and shipping it back over an SSL connection to the end user's browser. The devil is in the details, but it's pretty easy to understand.

Things get complicated when you start talking about anything other than a Web page. The next step up in complexity involves application translation. A good example of this is how SSL VPN devices treat file servers. The SSL VPN device will talk the native file server protocol, such as Microsoft's CIFS or FTP. But the application protocol is translated by the SSL VPN device from FTP or CIFS on the inside, to HTTP and HTML on the outside so that the end user sees the file server as if it were a Web page, in effect "Webifying" the application.

Application translation works for some things, but not for others. Some applications, such as Microsoft Outlook or instant-messaging tools, have a particular look and feel that is lost during the translation to a Web-based interface. This brings us to port forwarding, a technique that works for well-defined applications. Port forwarding requires a very small application that runs on the end user's system, often a Java or ActiveX tool. The port forwarder listens for connections on a port that are defined for each application. When packets come in on that port, they are tunneled inside of an SSL connection to the SSL VPN device, which unpacks them and forwards them to the real application server. To use the port forwarder, the end user simply points the application he wants to run at his own system rather than the real application server.

Port forwarding is a very effective technique, but it also has some severe limitations. For port forwarding to work, the applications need to be well-behaved and predictable in their network connectivity patterns and needs. Although there are port-forwarding tools written in Java that work across platforms, our experience was that port forwarders tend to be platform-specific.

The fourth technology some vendors are including in their products is network extension. SSL VPN network extension connects the end user's system to the corporate network, with access controls only based on network-layer information, such as destination IP address and port number.

Network extension also moves completely away from operating system independence and requires administrative access to the local system. SSL VPN network extension runs on top of the SSL protocol, trading off the higher security of IP Security for simplicity of management and greater robustness in the face of different network topologies, such as firewalls and network address translation.

— Joel Snyder

Unix FTP server, both worked perfectly. But when we aimed them at our OpenVMS server, neither could hack it.

Our last series of tests looked at the port forwarding and network-extension capabilities. We maintained a strict rule about technical support: None was allowed.

Macintosh users be warned: Even the products that claim to work with Macintosh systems (NetScreen and Nokia say they support Mac OS X for port forwarding) don't fully hit the mark. We got NetScreen to work with one of our three Macintosh browsers, Safari, but we never could get Nokia to start properly.

For Windows users, port forwarding — where supported — works pretty well. We had no problems getting F5, NetScreen, Nokia and Symantec to forward single-port and multi-port applications. Whale hiccuped, refusing to run in the Netscape browser and claiming that a user needs to be a "Power User" to start the port forwarder. That would be reasonable, except that we were logged in as Administrator.

We hit glitches on the network extension front, too. While NetScreen and Netilla ran flawlessly, AEP wouldn't support the User Datagram Protocol (UDP)-based application we tried. F5 worked sometimes but other times we got a blue-screen on Windows 2000. Symantec's VPN also had problems, largely because there's no documentation and no client.

Based on our interoperability testing, we conclude that these products fall short of the promise of an easy-to-use universal gateway to enterprise applications. Simple Web pages and basic JavaScript seem to work pretty well in the better products, but we were disappointed that Java, Flash, file services, port forwarding and network-extension support were haphazard, difficult to work with and not interoperable.

Hitting on interoperability

This chart shows how each product fared against our application interoperability tests across all seven platform/browser combinations. 100% means all applications worked on all platforms. These percentages take into account lack of support as stated by vendors and interoperability failure in our tests. To get the most information out of this chart, find the application category you care about most and compare products in that column.

	Basic Web	Mail	Advanced Web	File services	Port forwarding and network extension
AEP	60%	75%	0%	0%	13%
F5	97%	64%	11%	72%	38%
NetScreen	100%	39%	11%	78%	63%
Netilla	73%	29%	0%	11%	25%
Nokia	100%	86%	0%	61%	63%
Symantec	94%	71%	11%	28%	38%
Whale	93%	36%	0%	22%	13%

Access control counts

As security appliances, these products need to provide fine-grained control of security of applications.

All products included the ability to enable and disable access to applications using groups. At the simplest end of the spectrum are AEP, F5 and Netilla. Netilla lets the network manager define a Web application as a series of URLs. Once the application is defined, users and groups are given or denied access to it. AEP has a similar level of control. F5 comes at the access control from the group level, but because of the way the interface is designed, you are actively discouraged from having more than a small number of groups, and users can be in only one group. In some environments, just saying "yes" or "no" at the application level is fine, but you can run out of options quickly.

With Symantec, rather than apply access controls to applications, you can apply access controls to groups and users. Thus, you say what a group has access to and easily manage many different groups and their access controls. In Symantec's hierarchical model, it's easy to say that engineers can read and write files from the file server, but QA testers only can read those same files. That sounds easy, but only Symantec and NetScreen let you think that way. Symantec's model is powerful. There are a lot of complexities to what you can do, but the product doesn't make it hard to get started as it has a good GUI front end.

Another dimension to access control is going further than just group or user. In this regard, Nokia is the undisputed champ, although NetScreen and Whale also have some pieces of the big picture. For Nokia, the fine variations lie in what resources you have access to and what you can do with those resources. If you want to use a coarse control, you can pick groups that are permitted or denied access to a resource. But amazing control is just a click away. For example, you can permit access to a particular file if someone has authenticated using a Lightweight Directory Access Protocol (LDAP) server and his virus scanner is up to date.

Whale throws a change-up when it comes to access control. While providing simple access controls, the strength of this product lies in its application-level firewall. Whale lets you dissect individual URLs and provide a high level of error checking and validation. For example, in a URL that submits data to a form, Whale can check each attribute that should be in the form for length, blocking malformed data. It sounds tedious, complicated and hard to use, and it is. Whale helps out the network manager by prepackaging some of the most popular applications with pre-built rules sets. Unfortunately, for the applications we tested (Outlook 2003 and iNotes), neither rule set was current or correct. The only way we got those applications to work was by disabling the firewalling the product offers. Whale offered to fix its rule sets, saying that it would do this for any customer and any application.

A major disappointment in access control is how SSLVPNgateways control access to file servers. Whale and Netilla had unacceptably poor control of access. With these products, once a user is let in to a share on the Windows network, the SSL VPN gateway offered no additional control over where he could go or what he could do. In contrast, NetScreen, Nokia, and Symantec let you define read and write access at the individual file level. F5 also impressed us by including a virus scanner, which lets you scan files for infections during upload.

Authentication integration

Identifying users and putting them into groups is a critical part of any SSL VPN deployment. We tried to consider large businesses and the infrastructure they would already have in testing these products. We focused on LDAP and RADIUS as the most likely candidates for authentication and turned up good and bad designs (see graphic on page 6).

RADIUS was an easy choice because of widespread availability of RADIUS servers and the common use of RADIUS to authenticate against Windows, Unix and token-based systems such as RSA Security's SecurID, but we found that some vendors haven't done their homework on RADIUS. We linked all the products to our RADIUS server without problems, but only NetSscreen and Nokia were flexible enough to get group information out of the RADIUS server. In other products, RADIUS users had to be mapped to groups via some other method. In the worst case, Whale and AEP require you to manually map RADIUS users to the groups.

For many vendors, LDAP support is synonymous with Active Directory support. We had so many problems with AEP, Symantec and Whale that we had to replace our existing LDAP server for an Active Directory server to make them work. Even then, we continued to have problems with Symantec's LDAP implementation, including poor connectivity and obscure error messages.

If you are using LDAP in any other form, you'll want to go with F5, NetScreen or Nokia. We managed to trip up NetSscreen and find an LDAP configuration it couldn't handle, but technical support had a fix for it. All three of those products had sufficiently generic LDAP implementations to work with a variety of environments and schemas.

Because SSL, in general, is based on certificates, we expected these products to be excellent in their support of public-key infrastructure (PKI). But we were disappointed because only Nokia supported certificates for authentication (and even then didn't include support for Certificate Revocation Lists, which are required for any good PKI implementation).

F5, NetScreen and Whale did make use of client-side certificates for additional authentication, but not as a primary authentication method. For example, Whale has the concept of a "trusted endpoint," a user who not only authenticates but also presents a certificate. In defining access control in Whale's configuration, you can differentiate between users who have a certificate and those who don't. The idea is that a user will log on from home, at his home PC, and have his certificate; because he is trusted, he can be given a higher level of access than when he logs on from someone else's PC or an Internet kiosk, where his certificate won't be present. F5, NetScreen and Nokia all offer a similar configuration option.

Reporting and logging

As security appliances, we expected these SSL gateways to have strong auditing, logging and reporting features. We wanted to see audits of every change to the configuration. We wanted session data, showing when users logged on, logged out and how much resource they had consumed. And we wanted transaction data, every single Web page going through the system, if not for accounting then at least for debugging and usage analysis.

F5 exceeded our expectations. In addition to all the logging we wanted, the F5 gateway also was smart enough to automatically push its logs up to a server somewhere else, using FTP, SMTP or a secure copy. NetScreen, Nokia and Symantec all gave acceptable levels of logging with some associated bells and whistles. Nokia had more than a dozen subsystems that you could individually change logging on, or you could pick particular users and applications and increase the level of logging either for debugging purposes or just to keep a closer eye on parts of the system. This was a nice enterprise-level feature, where it might not be practical to turn up high logging on a production system just to help catch one problem.

Getting the log files off of the SSL VPN gateway is always going to be a bit tricky. We were disappointed that no one included RADIUS accounting, even though everyone used RADIUS for authentication. Some systems, such as NetScreen and Symantec, naturally wanted to push logs up using SYSLOG.

Net Results

RATING **4.5** WORLD CLASS WINNER

NetScreen-SA 5000 v3.3

Company: NetScreen Technologies, www.netscreen.com **Price:** $50,000. **Pros:** Strong authentication and access control features; many "thin client" options to support cross-platform users; innovative mail pass-through authentication; good control over SSL security settings; network extension more controllable than most. **Cons:** Reporting moderately weak; cache cleaner unacceptably slow; no FTP support.

RATING **4.4**

Nokia Secure Access System v1.1

Company: Nokia, www.nokia.com **Price:** $55,000 as tested. **Pros:** Outstanding fine-grained access control; very good authentication support including certificates and group-mapping features; very smart break-in/evasion features. **Cons:** Having two management interfaces can be confusing; logging via IPSO system is painful; lacking content-sensitive help; sparse GUI; portal support poor.

RATING **3.9**

FirePass Controller 4000 v4.0.2

Company: F5 Networks, www.f5.com **Price:** $24,990 as tested. **Pros:** Broad range of applications and authentication methods supported; delegated management; outstanding reporting/logging; virus scanning on uploads. **Cons:** Access control not finely grained; groups difficult to configure.

RATING **3.8**

Symantec Clientless VPN Gateway v4.0.2

Company: Symantec, www.symantec.com. **Price:** Starts at $9,500. **Pros:** Excellent access control model and configurability; real-time status and management very well done. **Cons:** More bugs throughout than most other products; good thinking in many areas clouded by brittle implementation; Layer 2 VPN is poor.

RATING **3.3**

Netilla Secutiry Platform v4.0.1

Company: Netilla Networks, www.netilla.com **Price:** $30,000 as tested. **Pros:** Outstanding support for terminal-based applications; additional network-layer firewall and DHCP features; session shadowing for support; add-ons to Windows Terminal Services, such as printer support; great documentation. **Cons:** No LDAP support; access control not finely grained; management GUI is slow.

RATING **3.3**

e-Gap Remote Access Appliance v2.5

Company: Whale Communications, www.whalecommunications.com **Price:** Starting at $23,000. **Pros:** Application-layer firewall provides extensive control. **Cons:** Management system complex and lacks central control; highly Windows-centric reduces compatibility with other authentication schemae; documentation needs significant improvement.

RATING **3.0**

AEP SureWare A-Gate AG-600 v2

Company: AEP Systems **Price:** $9,000 as tested. **Pros:** Small form factor; built-in terminal services application translation. **Cons:** Very limited application support; poor configuration capabilities; start-up configuration insecure by default; weak auditing/logging; no internal portal.

The breakdown

	WORLD CLASS Winner NetScreen	Nokia	F5	Symantec	Netilla	Whale	AEP
Application support 30%	4.5	4	4	3.5	4	3	3
Access control 30%	4.5	5	3	4	3	3.5	3
Interoperability 25%	4.5	4	4.5	4	3	3	3
Authentication 10%	4.5	5	4	3.5	3	4	3.5
Logging and reporting 5%	4	4	5	4	3	3	2
TOTAL SCORE	4.5	4.4	3.9	3.8	3.3	3.3	3.0

■ **Scoring Key: 5:** Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Consistently subpar

Without careful planning, this would overwhelm a normal SYSLOG server, mixing error messages with accounting information. Symantec has a good answer: It lets you pick different SYSLOG hosts for different services. Network managers might prefer to simply pull accounting data off the appliances themselves using a script, which is how Nokia and Whale serve it up.

We were also interested in real-time information. Although F5 had an excellent showing in this area, Symantec also won our admiration for its graphics and reporting, not only showing who was logged on, but also how the system itself was performing. A dashboard showing multiple graphs would have been a nice addition, but knowing what the CPU, memory and I/O load are will be great for any network manager who has to worry about performance. Netilla had a similar graphing capability for performance data. Whale caused us some concern because its real-time information tools didn't seem to work correctly. Even during the light load our testing presented, we could see that some events were being lost out of the real-time displays.

Handling authentication

Most products cover the main bases, but there are subtle differences in the details. This chart only indicates claimed support, not the results of our interoperability testing. In our tests, LDAP is a particular problem because of the variation in databases, so check compatibility with your schema carefully.

	RADIUS	LDAP	Digital certificates	Local user database	Windows
AEP	Yes (user only)	Yes	No	Yes	Yes
F5	Yes (user only)	Yes	No (add-on)	Yes	Yes
NetScreen	Yes (user & group)	Yes	No (add-on)	Yes	Yes
Netilla	Yes (user only)	No	No	Yes	Yes
Nokia	Yes (user & group)	Yes	Yes	Yes	Yes
Symantec	Yes (user only)	Yes	No	Yes	Yes
Whale	Yes (user only)	Yes	No (add-on)	No	Yes (may be local)

The (add-on) notation means that while you cannot use certificates for authentication, you can use them to supplement other authentication methods.

Picking a product

It's difficult to pick an obvious favorite. While we were not overly excited by the AEP, Netilla or Whale offerings overall, each has its own strengths. Whale includes a sophisticated application layer firewall. Netilla has the most extensive set of application translation functions. However, these products looked more like they had been wedged into the SSL VPN gateway space and will be most appropriate when application requirements call for their specific strengths.

F5 holds our admiration for its easy-to-use interface and strong product. But it seems particularly weak in access control, something the product management team told us it is working on for future versions.

The NetScreen, Nokia and Symantec development teams all had done serious thinking about SSL VPNs from scratch, and their products are sprinkled with bits and pieces showing that they have spent a fair amount of time in the trenches getting this to work and understanding the tough issues.

Snyder is a senior partner at Opus One in Tucson, Ariz. He can be reached at joel.snyder@opus1.com.

www.nwfusion.com

More online!

Online Buyer's Guide

Detailed product information from 15 vendors.

DocFinder: 9231

Thanks

Thanks to all the vendors that loaned us software and hardware to complete this review. Those include Apple, for loan of a Powerbook for client tests; Avocent, for loan of an AMX KVM switch; Macromedia, Altio, IBM, Microsoft, Ipswitch and Citrix for assisting with installation and configuration of their applications; and VMware (soon to be EMC) for use of GSX Server to run multiple applications.

Global Test Alliance

■ **Snyder** is a member of the Network World Global Test Alliance, a cooperative of the premier reviewers in the network industry, each bringing to bear years of practical experience on every review. For more Test Alliance information, including what it takes to become a member, go to www.nwfusion.com/alliance.